REMARKS

Claims 2, 4-6, 11, 13-14, 16-18 and 21-24 have been canceled above. Claims 25-37 have been added. The original claims were rejected under 35 USC 103 based on Goldfeder et al. and Turkboylari. Applicants respectfully traverse this rejection based on the following.

Amended claim 1 recites a computer implemented method for evaluating a security risk of an application. A determination is made whether the application is shared by different customers. A determination is made whether a third party can have unauthorized administrative authority to data maintained by the application. A determination is made whether a third party can have unauthorized read and/or write access to data maintained by the application. A numerical value or weight is assigned to each of the foregoing determinations. Each of the numerical values or weights corresponds to a significance of the respective determination in evaluating the security risk. The numerical values or weights are combined to evaluate the security risk.

Goldfeder et al. disclose evaluation of a security risk associated with loading an application. "For instance a virus evaluator may be configured to examine each component of an application for the possibility that the application contains a virus." Goldfeder et al. Paragraph 0035. "For instance, a scoring engine may have determined that the application has requested sufficient permissions to read and modify files on the computer, and to transmit data over a network connection. Based on that information, together with perhaps other evidence, a privacy evaluator may have determined that the application is likely to share the user's information over the network." Goldfeder et al. Paragraph 0039. Thus, Goldfeder et al. disclose virus scanning. Goldfeder et al. also disclose an analysis of an application to determine whether the application itself is malicious, i.e. likely to have accessed files and improperly transmitted file data over a network. In contrast, the present invention determines if an application is vulnerable to some type of attack. Moreover, Goldfeder et al. do not disclose or even suggest any of the three determinations recited in amended claim 1, nor the use of such determinations in evaluating a security risk.

Turkboylari discloses a secure computing environment using a secure bootloader, shadow memory and protected memory. "Operators of computer systems are rightfully concerned about the security of electronically stored information from unauthorized access, especially regarding sensitive and valuable business information. Also as is well known in the art and by the general public, malicious attacks of computer systems by way of computer viruses, and also by way of unauthorized access to computer networks, are also of significant concern." Turkboylari Paragraph 0004. However, Turkboylari does not disclose or even suggest the first two determinations recited in amended claim 1, nor the use of such determinations in evaluating a security risk.

Claims 3, 7-10, 12, 14-5 and 19 depend on claim 1, and therefore, distinguish over Goldfeder et al. and Turkboylari for the same reasons that claim 1 distinguishes thereover.

Independent claim 25 distinguishes over Goldfeder et al. and Turkboylari for the same reasons that amended claim 1 distinguishes thereover.

Claims 26-31 depend on claim 25 and therefore, distinguish over Goldfeder et al. and Turkboylari for the same reasons that claim 25 distinguishes thereover.

Claim 32 recites a computer program product for evaluating a security risk of an application. First program instructions determine whether a vulnerability in the application can be exploited by a person or program which has not been authenticated to the application or a system in which the application runs. Second program instructions determine whether a third party can have unauthorized administrative authority to data maintained by the application. Third program instructions assign a numerical value or weight to each of the foregoing determinations. Each of the numerical values or weights corresponding to a significance of the respective determination in evaluating the security risk. Fourth program instructions combine the numerical values or weights to evaluate the security risk.

As noted above, Goldfeder et al. disclose virus scanning. Goldfeder et al. also disclose an analysis of an application to determine whether the application itself is malicious, i.e. likely to

have accessed files and improperly transmitted file data over a network. In contrast, the present invention determines if an application is vulnerable to some type of attack. Moreover, Goldfeder et al. do not disclose or even suggest either of the determinations recited in claim 32, nor the use of such determinations in evaluating a security risk.

Turkboylari discloses a secure computing environment using a secure bootloader, shadow memory and protected memory. "Operators of computer systems are rightfully concerned about the security of electronically stored information from unauthorized access, especially regarding sensitive and valuable business information. Also as is well known in the art and by the general public, malicious attacks of computer systems by way of computer viruses, and also by way of unauthorized access to computer networks, are also of significant concern." Turkboylari Paragraph 0004. However, Turkboylari does not disclose or even suggest either of the determinations recited in claim 32, nor the use of such determinations in evaluating a security risk.

Claims 33-37 depend on claim 32 and therefore, distinguish over Goldfeder et al. and Turkboylari for the same reasons that claim 32 distinguishes thereover.

Based on the foregoing, the present patent application as amended above should be allowed.

Respectfully submitted,

Dated: 02/01/2007
Telephone: 607-429-4368
Fax No.: 607-429-4119

//Arthur J. Samodovitz//
Arthur J. Samodovitz
Reg. No. 31,297